REMARKS

In response to the Office Action mailed on <u>March 21, 2008</u>, Applicant(s) respectfully request(s) reconsideration.

Claims 1-42 are now pending in this Application.

In this Amendment, claims 1, 5, 10, 19, 21, 39 and 41 have been amended and claims 4, 6 and 40 have been cancelled and claims 42-44 have been added. Claims 1, 21, 39, 41 and 42 are independent claims and the remaining claims are dependent claims Applicant(s) believe that the claim(s) as presented are in condition for allowance. A notice to this affect is respectfully requested.

Claims 1-41 have been rejected under **35 U.S.C. §103(a)** as being obvious over Moriconi, U.S. Patent No. 6,941,472 (hereinafter Moriconi '472) in view of Lunt, IDES: A Progress Report (hereinafter Lunt).

Lunt, however, cited for the proposition of disclosing comparison to a set of preexisting allowable accesses, does not show, teach, or disclose comparison to a determined structure of the access attempt, as now discussed in further detail. Claim 1 has been amended with the subject matter of claim 4, to clarify that

> comparing the access attempt to preexisting access attempts comprises:
>   determining a structure of the access attempt corresponding
> to a syntactical structure of the access attempt; and
>   comparing the determined structure of the access attempt
> independently of the data values implicated in the access attempt.

The Office Action suggests that Lunt teaches the claimed syntactical arrangement structure at page 6, col. 2, however the Lunt approach employs ordinal and categorical measures. Each of the Lunt measures, therefore, is unary in that it indicates the occurrence (via a numerical score) of a quantifiable aspect of observed behavior. In contrast, the claimed syntactical arrangement denotes a structure or position of multiple elements defined by the syntax. As is known in the art, such a syntax includes rules specifying certain subsets of elements that may precede or follow other elements. Accordingly, merely

counting the occurrence of a Lunt item (e.g. CPU time, records produced) differs because the Lunt item does not encompass the context in which a counted item occurs, in contrast to the claimed syntactical structure. Claims 21, 39 and 41, rejected on similar grounds, have been likewise amended.

The Office Action further suggests that Lunt teaches comparison to previous access attempts., at col. 2. Lunt, however, discloses a user's historical profile of activity (col. 2, 1st full para.), and clarifies this at col. 3, 2nd full paragraph, characterized as detecting "when a secretary is not behaving like a secretary." Nowhere in Lunt, alone or in combination, is shown, taught or disclosed the use of a computed hash on previous access attempts, as taught by the present invention. Accordingly, claims 21, 39 and 41 has been further amended with the subject matter of claim 6, to clarify that

> determining the structure further comprises:
> parsing the access attempt; and
> building a parse tree from the parsing, the parse tree
> indicative of a syntactical structure of the data access attempt,
> wherein comparing further comprises computing a hash value from
> the parse tree, and comparing the hash value to the hash values of
> previous access attempts

The Office Action further suggests that Lunt teaches the claimed structure of the access attempt as a categorical intrusion measure (p. 6). Lunt, does not show, however, that the claimed structure includes building a parse tree indicative of the attempt. (claim 6).

Claims 21, 39 and 41, similar in scope to claim 1, have been therefore amended with the subject matter of claims 4 and 6, to clarify the distinguishing features discussed above The Office Action suggests that Allen '625 teaches the claimed hash tree based on the syntactical structure, however Allen '625 shows a hash employed for data ACCESS, not for data COMPARISON. Allen, therefore, offers a hash table as an alternative to storing the data in a parse tree (col. 12, lines 9-14). Thus, it is the information in the individual parse tree nodes that are hashed in Allen, for facilitating access to a particular node as an alternative to a tree traversal. The hash refers to accessing a particular node

rather than traversing the tree, not the claimed approach of a hash value representative of multiple (or all) values in the tree for comparison with other hash values of other trees.

In contrast, the claimed hash is a hash computed from the entire structure (page 8, line 28-page 9 line 4). In other words, Allen '625 shows a separate hash for each node in the tree, while the claimed approach generates a hash covering the entire tree. Further, the hash in Allen has a completely different usage- for accessing nodes in the tree via a hash value, rather than traversal, as is known in the art of computer data structures. The claimed hash is for comparing the tree structure to OTHER tree structures to assess similarity.

This distinction is further clarified in added claim 42, which recites, inter alia, computing a hash value from the parse tree, the parse tree deterministic of a query structure of the access attempt such that similar access attempts share the query structure.

Further, one of skill in the art would not look to Allen '625 to modify Moriconi '472 or Lunt because Moriconi and Lunt teach intrusion detection, while Allen discloses only data conversion. Thus, Allen '625 is directed toward solving an entirely different type of problem, specifically converting data from a central server for multiple recipients, therefore broadening access, while the intrusion detection system strives to narrow access.

Claim 42 has been herein added, to further clarify and distinguish particular features of Applicant's claimed invention, including employing a learned baseline and capture mode for building (augmenting) the baseline from successive accesses, as disclosed at page 4, lines 1-11. Access attempts are compared to a baseline built from both rule based access policy and generated suggested rules, as disclosed at page 8, lines 21-27.

The claimed parse tree depicts a syntactical arrangement defined by a parseable syntactical structure expressible as a binary tree, taught at page 18, lines 17-26, and that the resulting hash values are deterministic of similar SQL statements in successive access attempts, as discussed at page 9, lines 1-5.

These distinguishing features are not shown, taught, or disclosed in Lunt or Moriconi, alone or in combination, and accordingly, claim 42 is likewise deemed allowable for the reasons given above.

Claim 43 has been added to further clarify that comparing the determined structure of the access attempt is performed independently of the data values implicated in the access attempt, such that the computed hash is unaffected by differences in queried data values, further refining the subject matter of claim 4.

Claim 44 has been added to further clarify augmenting the current baseline by identifying a sampling window of access attempts, the sampling window deterministic of allowable access patterns to the protected resource, storing an indication of the access attempts made during the window of access attempts, and merging the window of access attempts with the current baseline set of access attempts, the current baseline deemed deterministic of allowable access behavior, to clarify the feature of continuously building the baseline with successive access attempts, refining claim 44 with features of claim 15. Such features are not shown, taught, or suggested in the cited references.

Claim 39 has been further amended for **§101** rejections, and claim 40 cancelled.

As the remaining claims depend, either directly or indirectly, from claims 1, 21, and 42, it is respectfully submitted that all claims are now in condition for allowance.

Applicant(s) hereby petition(s) for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an online payment made herewith, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,

___/CJL/_____
Christopher J. Lutz, Esq.
Attorney for Applicant(s)
Registration No.: 44,883
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive, Suite 280
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: GRD03-03

Dated: July 21, 2008